Proof of retrievability

Presenter: Melek Önen
Contact: melek.onen [at] eurecom.fr

Abstract: Nowadays, data outsourcing, that is delegating one's computing to external parties, is a well- established trend in cloud computing. Along with unprecedented advantages such as lower cost of ownership, adaptivity, and increased capacity, outsourcing also raises new security and privacy concerns in that critical data processing and storage operations are performed remotely by potentially untrusted parties. In this talk, we focus on data retrievability, a security requirement akin to outsourced data storage services like Dropbox, Amazon Simple Storage Service. Data retrievability provides the customer of a storage service with the assurance that a data segment is actually present in the remote storage. We propose an efficient proof of retrievability (POR solution) that achieves high reliability assurance with low communication and computational cost at the client side by combining a privacy-preserving word search algorithm suited to large datastores like cloud storage systems with randomly-valued watchdogs that are inserted in data segments.